

PREPARED REMARKS FOR DELIVERY
FCC CHAIRMAN JULIUS GENACHOWSKI
WHITE HOUSE CYBERSECURITY PUBLIC-PRIVATE
PARTNERSHIP INITIATIVES ANNOUNCEMENT
MAY 30, 2012

Thank you Howard Schmidt for inviting me here today. More important, congratulations on your retirement and thank you for your service. Howard was the first person to serve as Cybersecurity Coordinator for the White House. The position itself reflects the need for a coordinated interagency effort to tackle this challenge.

The steps we've taken to increase security at both at the FCC and by the IBG are testaments to the terrific job Howard has done.

Speaking of the FCC's work, thank you to Glen Post.

Ensuring the security and reliability of commercial networks has long been at the core of the FCC's mission. Years ago, we stood up an expert advisory panel called the Communications Security, Reliability and Interoperability Council – what we call CSRIC. In fact, an earlier iteration of CSRIC became one of the first federal entities to develop cybersecurity best practices – back in 2001.

Over the last year, Glen led CSRIC's cybersecurity working groups, which have delivered practical solutions to specific problems, solutions that will materially improve the security of our broadband networks.

Thank you, Glen.

Howard and Glen's work highlights a few key points about the cybersecurity challenge.

Cyber attacks are a new kind of threat. And tackling them requires a new kind of approach.

First, addressing cyber threats requires the commercial communications ecosystem to engage in a way that's different than other threats. Private networks are of course a major part of Internet communications. And so we need the private sector to proactively engage on this issue.

Second, addressing cyber threats requires interagency collaboration. Different agencies have different areas of expertise and responsibilities relevant to tackling Cybersecurity.

A third key point is that in tackling cyber threats, we need to do it in a way that preserves the ingredients that have fueled and will fuel the Internet's growth and success.

That means solutions that preserve Internet freedom and the open architecture of the Internet, which have been essential to the Internet's success as an engine of innovation and economic growth.

Privacy is a similarly vital principle. Privacy and security are complementary – both are essential to consumer confidence in the Internet and to adoption of broadband.

Another key component for problem-solving in this area: the multi-stakeholder model.

The history of the Internet tells us that the multi-stakeholder model can produce solutions.

This is the approach we've taken at the FCC – and it is also the approach the IBG is taking.

I'm pleased that DHS and NIST have partnered in the FCC's work. And I'm pleased that the FCC has participated in the IBG process.

And the important thing is that this approach is delivering results.

In March, CSRIC's botnet working group presented a practical, voluntary U.S. Anti-Bot Code of Conduct, or ABC, to reduce the threat of bots in residential broadband networks. And ISPs representing nearly 90% of US Internet subscribers have committed to implementing the Code of Conduct.

The ABC provides for improved detection by ISPs of bots in their customers' computers, and to notify consumers when their computers have been infected.

And it provides for making tools available to help remediate bots.

The ABC also includes steps to educate consumers so that they can look for signs that their computers have been infected.

I am proud of this joint industry and FCC effort, which also included steps on DNS-SEC and IP Route Hijacking. I also recognize that it represents one facet in what must be a multi-pronged approach to botnet remediation, which must extend to include others in the ecosystem – and botnets are just one part of the broader cyber challenge.

But with private sector engagement, interagency collaboration, and a commitment to the principles that have fueled the Internet's success, I am confident we can make a real difference in increasing the security of the Internet and harnessing its enormous opportunities.

Thank you.